Detection and Prevention of DDOS attack using SDN for E-banking system

Bhushan Bhonkar[1], Nishant Mehta[2], Rahul Gaikwad[3], Amit Kumar[4], Madhavi Darokar[5]
[1, 2, 3, 4, 5] Department of Computer Engineering
[1, 2, 3, 4, 5] JSPM's Imperial College of Engineering and Research, Pune, India

Abstract- *In the current world the most important threat to servers across the world is Denial of Service attack. DDOS attack often target web based services hosted on high profile servers such as banks or credit card payment gateways. A DDOS attack is analogous or similar to multiple groups of people crowding the entry door or a gate to a shop or business and not letting legitimatize parties enter into the shop or business disrupting normal operations. There is a distinct need of such an application to stop multiple attacks on the system. These attacks originate from a singular point of contact. Being DDOS creates a massive flood of users which can extensively break the system and stop its functioning. This survey paper constitutes in depth study of the problems seen by multiple banks and card based businesses. The major problem seen in banks and their response on the same is studied in depth to provide the required solution to these problems*

Keywords- DDOS, Multiple attack prevention, Banking application, SDN.

I. INTRODUCTION

Denial of service attack programs have been around for many years with growth of internet they have increased. A DDOS streams do not have common characteristics as the currently available intrusion detection system (ids). The aim of DDOS attacks is to make internet based services unavailable to its legitimate users. DDOS attacks is challenging for two reasons. First, the number of attacks involved in DDOS attacks is very large. If the volume of traffic sent by single attacker is small then the victim host is overwhelming. Second, attacker usually spoofs IP address, which is difficult to trace. Three types of flooding attacks are accessed in it TCP/SYN, UDP & ICMP. TCP /SYN flood is a most dangerous of the DDOS attack. UDP flood attacks are to exploit the UDP services. UDP packets to different port of a target in random way. ICMP is a smurf attack which is used to put the target resources out of service that results in making the resource stagnate. DDOS attacks network follows two types of architecture. The agent handler architecture and internal relay chat.

The agent–handler architecture for DDOS attack is comprised of clients, handler and agents. The attacker communicates with DDOS client system. The handlers are often software packages located through the internet that are used by client to communicate with the agent.

The system which is being built will help to stop multiple attacks using SDN based protocols. The system will prevent multiple attacks like SQL injection, Brute force attack, URL injections and cross site scripting attack. Database will be encrypted to create a secure environment for the customers.

II. REVIEW OF RELATED LITURATURE

A. Internet based attacks .

There are multiple types of attacks which can be faced by the server and there is a distinct need to stop these web attacks. Hacking using exploits is seen to be major creation or root of these attacks. Every single day there are new exploits which are found by which identity of the users is compromised. New web based attacks coming out every day causes business, community and individuals to take security seriously. These revelations teach everyone the importance of basic security concepts. Multiple books, articles are available on the websites. There need to be credible information on these attacks and how one can protect himself from these attacks.

B. Conceptual framework

According to current trends as mentioned in the "Web site Hacked Trend Report Q2 2016 " by Sucuri Security, we see multiple platform are affected like Wordpress , Joomla by malware and exploits. Wordpress experienced a 4% drop from 78% in Quarter 1 to 74% in Quarter2. Joomla experienced a 2.2% increase from 14% in Quarter1 to 16.1% in Quarter2. These analysis indicate increase in malware and viruses in multiple web based servers. Identification of the attack is the primary focus of this project. The analysis indicate when the type of attack is known is become easier to stop and know exactly where this attack is coming from. When the type of attack is known defences can be mounted to

avoid data loss. There are multiple instances where attacks not detected in their early stages and thereby couldn't be stopped earlier. When attacks are not stopped quickly they tend to create damage and pose a greater threat to the system. Hence, there is a definite need for an application to stop the attack from ever occurring.

III. SYSTEM ARCHITECTURE

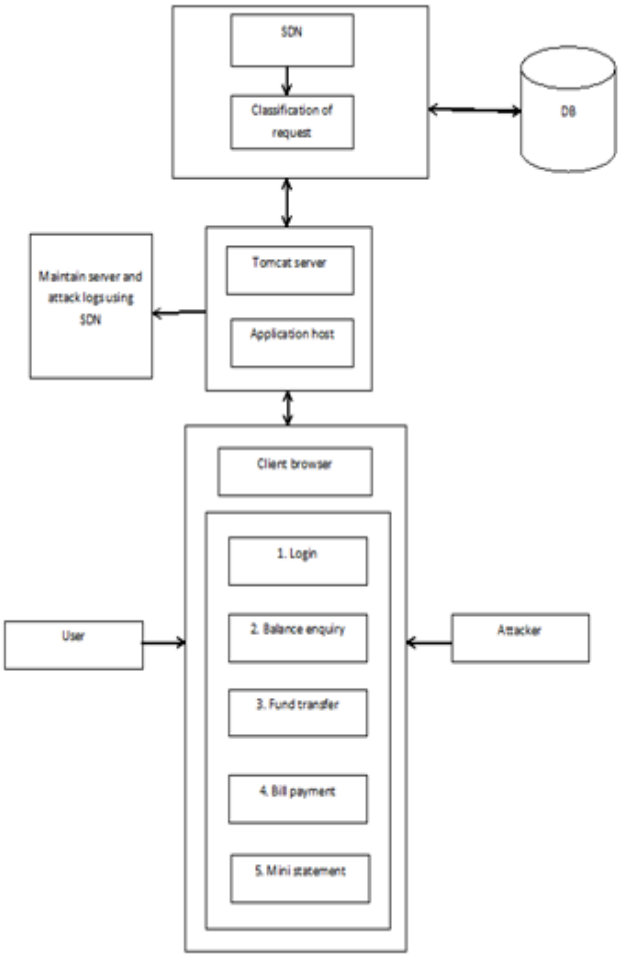


Figure 1.

The main purpose of the architecture is to provide privacy to the customers data and transaction

A. Interaction with banking personnel

To understand the exact requirement for banking based application we interacted with multiple employees of a private bank. Following are the generic requirement from these personnel:

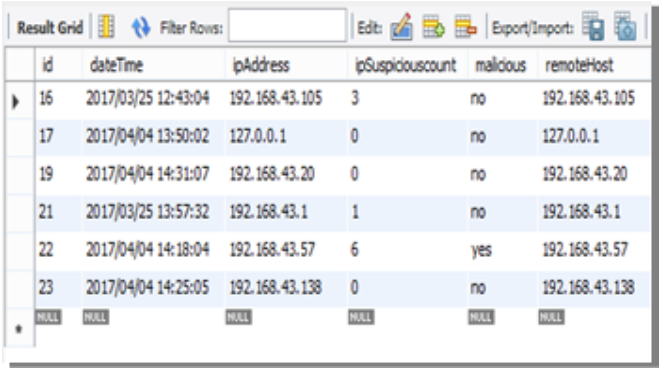
1. Implementation of security based application where web attacks are quickly discovered and stopped.
2. Personal information of the client get stored into the database in encrypted format.
3. Dynamic password is created and pin is generated and sent to user on mail.
4. The administrator can check detailed logs of attacks for analysis and studying the same.

B. Active users

Multiple users based could use the application to quickly perform any banking or any financial task. Here quality and integrity of information is of paramount importance.

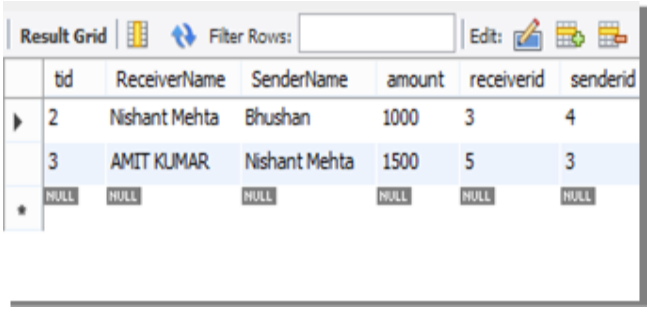
IV. WORKING MODEL

In modern era where digital system is common amongst the youths and the rest ones. This digital system is having proes and cons. Due to digitalization of the markets the era of hackers has also increased so security is major issues among the users. So we worked on an inovative idea of securing the e-banking with ddos attacks using sdn as a security service. In our project we have successfully prevented the attacks like ddos, sql attack, url injection against the e-banking systems. In our project we have used SDN(software defined network) which is acting as a guard to e-banking system. If you are a new user then our banking then registration page is their where you have to fill all your necessary details online, now after registration the request goes to the administrator for approval the administrator after verifying the details approves the request, after which your user name and password is sent to your respective email id. With your email id you can login and perform your transactions successfully. In our project sdn works as a filer, it filters all the requests from the user and give necessary details to the user and the administrator so that the administrator can take necessary steps for the safety of the users. If you logged in to your account and want to perform any attack for eg. let us consider you are trying to perform cross site attack. Let us take a simple example of cross site attack you are performing your transaction and you are trying to write some kind of scripts in your remark then it will be detected and it will be informed to both user and the administrator. If you are trying to perform sql injection while you are logged in to your account then also it will be detected and it will be informed to both user and the administrator.



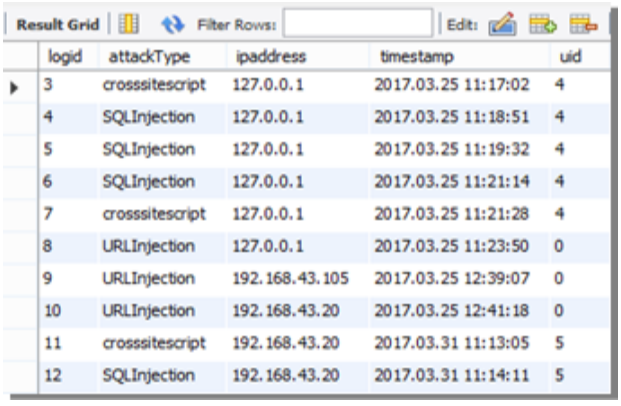
id	dateTime	ipAddress	ipSuspiciouscount	malicious	remoteHost
16	2017/03/25 12:43:04	192.168.43.105	3	no	192.168.43.105
17	2017/04/04 13:50:02	127.0.0.1	0	no	127.0.0.1
19	2017/04/04 14:31:07	192.168.43.20	0	no	192.168.43.20
21	2017/03/25 13:57:32	192.168.43.1	1	no	192.168.43.1
22	2017/04/04 14:18:04	192.168.43.57	6	yes	192.168.43.57
23	2017/04/04 14:25:05	192.168.43.138	0	no	192.168.43.138

Figure 2. Logs of Attack Detection



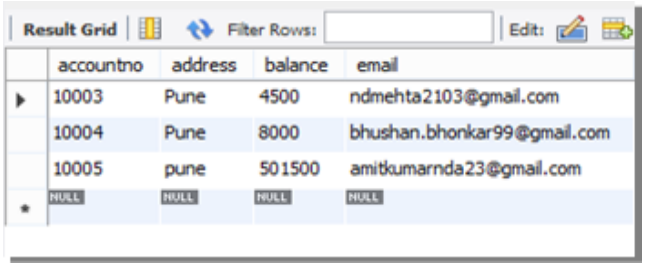
tid	ReceiverName	SenderName	amount	receiverid	senderid
2	Nishant Mehta	Bhushan	1000	3	4
3	AMIT KUMAR	Nishant Mehta	1500	5	3

Figure 3. Transaction



logid	attackType	ipaddress	timestamp	uid
3	crosssitescript	127.0.0.1	2017.03.25 11:17:02	4
4	SQLInjection	127.0.0.1	2017.03.25 11:18:51	4
5	SQLInjection	127.0.0.1	2017.03.25 11:19:32	4
6	SQLInjection	127.0.0.1	2017.03.25 11:21:14	4
7	crosssitescript	127.0.0.1	2017.03.25 11:21:28	4
8	URLInjection	127.0.0.1	2017.03.25 11:23:50	0
9	URLInjection	192.168.43.105	2017.03.25 12:39:07	0
10	URLInjection	192.168.43.20	2017.03.25 12:41:18	0
11	crosssitescript	192.168.43.20	2017.03.31 11:13:05	5
12	SQLInjection	192.168.43.20	2017.03.31 11:14:11	5

Figure 4. Detection and Prevention of DDOS



accountno	address	balance	email
10003	Pune	4500	ndmehta2103@gmail.com
10004	Pune	8000	bhushan.bhonkar99@gmail.com
10005	pune	501500	amitkumarnda23@gmail.com

Figure 5. User details

VI. TESTING

Testing is an important part of project life cycle. Testing is done basically to find out any bug in our project or any error, all the requirements of client are fulfilled or not. To find out this various test cases are applied to the deployed model. If our deployed model is working according to test cases then the result is analyzed. If result is positive then particular test case is true else it is false.

Testing is done on the basis of actual working model of system. The testing is done according to functional working, system compatibility, input and output to the system and performance of the system.

This Paper explains the various activities performed as part of Testing of "Secure Banking Application" using various test cases and UML representation.

Application Overview:

Our main motivation of application is to detect and prevent DDOS attack and various attacks like URL Injection, SQL Injection, and Cross-Site Scripting etc. in e-Banking Application and to make our system more confidential and secure for user purpose.

Testing Scope:

Testing performed on following scope:

a) In scope:

The actual functional testing is done in this scope. According to our system, functionality of system is – User registration, user approval, user login, various user transactions, Attack Detection and Prevention.

b) Out of scope:

In this scope, unwanted testing are not done/ performed.

c) Items not tested:

The items that are remained to test are under this scope. Basically third party systems are come under this scope. This items are tested under UAT i.e. User Acceptance Testing.

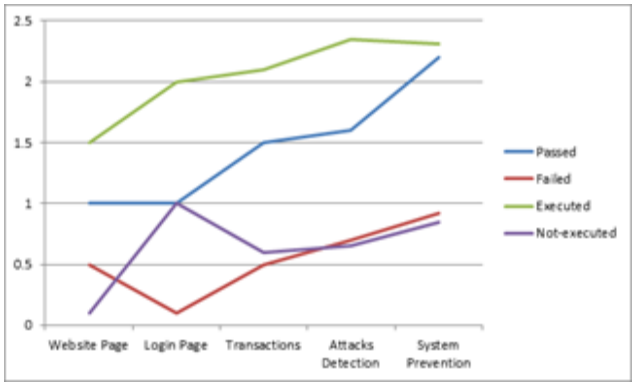


Figure 6. Testing of SDN

VII. CONCLUSION

Using this application we try to overcome multiple security problems and attacks which may lead to information and security leakages. A comprehensive work for protecting integrity of the information stored in the databases is a primary purpose for the application. Detection of multiple attacks will create a barrier for stealing or manipulating information in the system. Such a solution is an important breakthrough to effectively and efficiently stop the attacks.

VIII. ACKNOWLEDGEMENT

We thanks our colleagues who provided insight an expertise that greatly assisted the research.We thank our Prof. Madhavi Darokar inspiring us to do this projects and her comments in the manuscript.

REFERENCES

[1] https://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-shah.pdf

[2] https://sucuri.net/website-security/hacked-reports/Sucuri-Hacked-Website-Report-2016Q2.pdf

[3] https://securityintelligence.com/the-10-most-common-application-attacks-in-action/

[4] https://en.wikipedia.org/wiki/Software-defined_networking

[5] Y. Zhang, “An adaptive flow counting method for anomaly detection in sdn,” in Proceedings of the ninth ACM conference on Emerging networking experiments and technologies. ACM, 2013.

[6] “A covariance analysis model for ddos attack detection,” in Communications, 2004 IEEE International Conference on IEEE, 2004, by S. Jin and D. S. Yeung.

[7] S. Shin and G. Gu, “Attacking Software-defined networks: a first feasibility study,” in Proc. the second ACM SIGCOMM workshop on Hot topics in software defined networking, 2013

[8] Survey on DDOS attacks on E-Banking Systems , International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 11 by Bhushan Bhonkar, Nishant Mehta, Rahul Gaikwad, Amit Kumar, Madhavi Darokar